HW

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,491	01/04/2002	Christopher J. Frantz	COMP:0272 P01-3946	6228

7590 09/21/2005

Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER	
SMITHERS, MATTHEW	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/037,491	FRANTZ ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/15/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed April 15, 2002 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-7, 9-15, and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,223,287 granted to Douglas et al.

Regarding claim 1, Douglas meets the claimed limitations as follows:

"A remote server management controller, comprising:

a web server adapted to engage in encrypted communication over a first communication link (see column 3, lines 41-44; column 4, lines 20-28 and Figure 4, elements 43 and 46),

the web server being further adapted to receive and respond to a request for secret data from a client computer over the first communication link (see column 3, lines 51-54 ; column 4, lines 28-33 and Figure 4, elements 43 and 46),

the secret data being adapted to encrypt a second secure communication link (see column 3, lines 56-59); and

a remote console server adapted for operable communication with the web server, the remote console server being further adapted to engage in communication with the client computer over the second communication link, wherein the remote console server receives the secret data from the web server and uses the secret data to encrypt communication sent over the second communication link." see column 3, lines 54-65.

Regarding claim 2, Douglas meets the claimed limitations as follows:
"The remote server management controller of claim 1 wherein the secret data is a secret key." see column 4, lines 4-8 and column 4, lines 28-33.

Regarding claim 3, Douglas meets the claimed limitations as follows:
"The remote server management controller of claim 1 wherein the secret data is a random number that is used by the remote console server to generate a secret key." see column 4, lines 28-33.

Regarding claim 4, Douglas meets the claimed limitations as follows: "The remote server management controller of claim 2 wherein the remote console server is adapted to use the secret key to decrypt communications received over the second communication link." see Abstract, "The set of encryption information . . . efficiently encipher and decipher data".

Regarding claim 5, Douglas meets the claimed limitations as follows: "The remote server management controller of claim 1 wherein the request for the secret data is initiated by a remote console applet executing on the client computer, the remote console applet being adapted for operable communication with a browser application executing on the client computer, the remote console applet transmitting the request for secret data to the browser application, the browser application transmitting the request for secret data to the web server via the first communication link." see column 4, line 19 to column 5, line 41.

Regarding claim 6, Douglas meets the claimed limitations as follows: "The remote server management controller of claim 1 wherein the first communication link is between the web server and a browser application executing on the client computer." see Figure 4, element 43.

Regarding claim 7, Douglas meets the claimed limitations as follows: "The remote server management controller of claim wherein the second communication link is between the remote console server and a remote console applet executing on the client computer." see Figure 4, secured channel between elements 48 and 50.

Regarding claim 9, Douglas meets the claimed limitations as follows:

"A client computer, comprising:

a browser application adapted to execute on the client computer, the browser application being adapted to transmit a request for secret data to a remote server management controller across a first communication link (see column 3, lines 41-44; column 4, lines 20-28 and Figure 4, elements 44 and 43); and

a program adapted to execute on the client computer, the program being adapted to initiate the request for secret data and use the secret data to encrypt communication over a second communication link." see column 4, line 19 to column 5, line 41 and Figure 4, secured channel between elements 48 and 50.

Regarding claim 10, Douglas meets the claimed limitations as follows: "The client computer of claim 9 wherein the secret data is a secret key." see column 4, lines 4-8 and column 4, lines 28-33.

Regarding claim 11, Douglas meets the claimed limitations as follows: The client computer of claim 9 wherein the secret data is a random number that is used by the remote console applet to generate a secret key." see column 4, line 19 to column 5, line 41.

Regarding claim 12, Douglas meets the claimed limitations as follows: "The client computer of claim 9 wherein the program is adapted to use the secret data to decrypt information received via the second communication link." see Abstract, "The set of encryption information . . . efficiently encipher and decipher data".

Regarding claim 13, Douglas meets the claimed limitations as follows: "The client computer of claim 9 wherein the secret data is generated by a web

server in the remote server management controller." see column 4, line 19 to column 5, line 41.

Regarding claim 14, Douglas meets the claimed limitations as follows: "The client computer of claim 9 wherein the first communication link is between a web server in the remote server management controller and the browser application." see Figure 4, element 43.

Regarding claim 15, Douglas meets the claimed limitations as follows: "The client computer of claim 9 wherein the program is a remote console applet and the second communication link is between a remote console server in the remote server management controller and the remote console applet." see Figure 4, secured channel between elements 48 and 50.

Regarding claim 17, Douglas meets the claimed limitations as follows: "A method of employing a first communication link between a client computer and a managed server to upgrade a second communication link between the client computer and the managed server from clear to encrypted, wherein the first communication link is encrypted, the method comprising the acts of:

receiving a request for secret data from the client computer via the first communication link (see column 3, lines 41-44; column 4, lines 20-28 and Figure 4, elements 43 and 46),

transmitting secret data to the client computer across the first communication link responsive to the request (see column 3, lines 51-54; column 4, lines 28-33 and Figure 4, elements 43 and 46); and

using the secret data to encrypt communications sent via the second communication link." see column 3, lines 54-65.

Regarding claim 18, Douglas meets the claimed limitations as follows: "The method of claim 17 further comprising generating a secret key from the secret data." see column 4, lines 4-8 and column 4, lines 28-33.

Regarding claim 19, Douglas meets the claimed limitations as follows: "The method of claim 17, further comprising using the secret data to decrypt data received via the second communication link." see Abstract, "The set of encryption information . . . efficiently encipher and decipher data".

Regarding claim 20, Douglas meets the claimed limitations as follows: "The method of claim 17 wherein the recited acts are performed in the recited order." see column 3, lines 37-65.

32

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,215,877 granted to Matsumoto and further in view of "Applied Cryptography, Protocols, Algorithms, and Source Code in C", by Bruce Schneier.

Regarding claim 8, Douglas discloses everything as applied above (see claim 1), however, Douglas does not specifically teach using the RC4 transform for the encryption method. Douglas teaches using a stream cipher (SEAL) as his encryption method (see column 5, lines 42-55. Schneier teaches RC4 is a simple fast stream cipher that is commonly used for encryption purposes. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Douglas' method for establishing a secured communication channel over the Internet with the stream cipher RC4 because the algorithm is easy to code into memory which allows for faster generation of encrypted communications. [see Schenier, pg 398]

Regarding claim 16, Douglas discloses everything as applied above (see claim 9), however, Douglas does not specifically teach using the RC4 transform for the encryption method. Douglas teaches using a stream cipher (SEAL) as his encryption method (see column 5, lines 42-55. Schneier teaches RC4 is a simple fast stream cipher that is commonly used for encryption purposes. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Douglas' method for establishing a secured communication channel over the Internet with the stream cipher RC4 because the algorithm is easy to code into memory which allows for faster generation of encrypted communications. [see Schenier, pg 398]

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Curtis (U.S. patent 5,870,544) discloses a method for creating a secure connection between a client and a server.

B. Weinstein et al (U.S. patent 6,094,485) discloses a method for negotiating an encrypted session between a client using SSL and a server.

C. Matsumoto (U.S. patent 6,215,877) discloses a method for establishing a secure communication between a key management server and a client.

D. Sharma et al (U.S. patent 6,766,165) discloses a method for managing a mobile network.

E. Walker et al (U.S. 2003/0037250) discloses a method for securely accessing content server using dual encrypted paths.

F. Chen et al (US 2003/0046542) discloses a method for using a secret in a distributed computing system.

G. Want et al (US 2003/0114190) discloses a method for securely communicating data between devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137